Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

Response to Call for View's on Australia 2020 Cyber Security Strategy

Dr Tahiry Rabehaja[1], Dr Ryan Springall[1] and Denny Wan[2]

[1]Risk Frontiers, Level 8, 33 Chandos Street, St Leonards NSW 20165

[2]Security Express

(email contact: tahiry.rabehaja@riskfrontiers.com)

Overview

The Australian Government, through the Department of Home Affairs, has called for views in developing Australia's next Cyber Security Strategy.

Risk Frontiers' response to this request concentrates on Cyber Risk quantification and its application to cyber insurance. Cyber insurance is one component of broader cyber security risk assessments with a focus on delivering risk transfer products to companies at risk. Our submission focuses on what is required to improve the understanding and pricing of cyber-risk in order to improve the resilience of Australian businesses to cyber-attacks. We argue that cyber insurance is currently under-used/developed for Australia and there is a need for an industry database on cyber incidents to better understand frequency / severity relationships.

About Risk Frontiers

Risk Frontiers specialises in the assessment, pricing and management of catastrophe risks across the Asia-Pacific region, with specialist skills in catastrophe loss modelling. We help organisations within the global (re)insurance industry, infrastructure operators, government departments and emergency services.

Our research and expertise covers major hazards affecting the region including floods, tropical cyclones, storms, bushfires, heatwaves, sea-level rise, coastal erosion and earthquakes. We also work with communities to understand the human dimension of risk and policy implications.

In 2019, Risk Frontiers delivered updates to our Multi-peril Workbench with enhancements to our nationwide catastrophe loss models. We also continue the development of a cyber-risk model in partnership with the Optus Macquarie University Cyber Security Hub.

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

Our work with government encompasses a diversity of projects including understanding community risk perception, evaluation of resilience and recovery programs, research into catastrophic disasters and the development of resilience frameworks.

We also undertake bomb blast loss modelling for damage incurred by commercial buildings due to terrorist activities. This work is undertaken for the Australian Reinsurance Pool Corporation (ARPC), a statutory body created under the Terrorism Act 2003.

As a partner of the Australian Research Council Centre of Excellence for Climate Extremes, Risk Frontiers is well positioned to deliver the latest in climate change solutions to enhance our clients' decision making. Risk Frontiers are a service provider to the Bushfire and Natural Hazards Cooperative Research Centre.

In drafting this response, Risk Frontiers also sought the advice of Denny Wan, a cyber-security specialist with particular expertise in quantifying risks using the FAIR framework.

Risk Frontiers Response to Australia's 2020 Cyber Security Strategy

1. What is your view of the cyber threat environment? What threats should government be focusing on?
   No response

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
   No response

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?
   No response

4. What role should government play in addressing the most serious threats to institutions and businesses located in Australia?

   Response: Cyber Security is not simply a technological issue not can it be removed completely from any operation in an economically effective way . It is an inherent risk that is growing in importance as more commercial and government essential services are conducted using information technology. With the economic and efficiency benefits comes downside risks, with the most severe consequences ranging from financial loss to businesses, physical damage to private property and

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

infrastructure and psychological impact on individuals. As a risk, cyber security needs to be better understood before mitigation, response and importantly risk financing strategies can be developed and implemented. In particular, Risk Frontiers' submission argues for a better understanding of the role of insurance as a risk transfer mechanism and also as feedback mechanism to good risk culture through premium and policy language signals.

To accurately price risk, insurers require a robust quantitative understanding of frequency (how often) and severity (how much financial loss). This data is often obtained through years of claims data and experience dealing with natural catastrophes, for example. In the case of cyber risks this understanding is currently lacking. To overcome this deficiency will require strong and pragmatic leadership from the government to ensure a cyber-risk resilient Australian economy.

The USA is amongst the countries with well-developed cyber security laws and regulation. In addition, the US government actively encourages US businesses to implement robust cyber risk management and in particular promotes the addition of cyber insurance into their Enterprise Risk Management strategy. According to a 2018 Aon report[1], the current global cyber insurance market premium is estimated to sit between 4 and 5 billion US dollars with the US accounting for more than 80% of this market. Figure 1 shows the breakout of global cyber insurance premiums. The US market is what would be considered maturing while of the rest of the world is very much developing and expected to grow. In 2018, the Australian cyber insurance market premium was approximately $60 million US dollars, which was about 2% of the global market by premium volume.

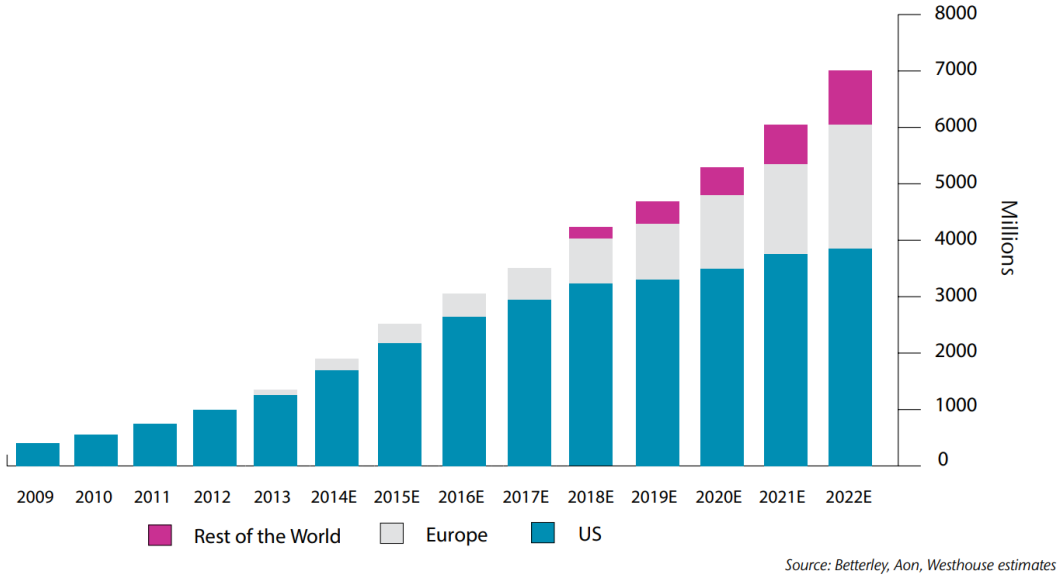

Figure 1: Measured and estimated written cyber insurance premiums. (Source: Aon Cyber Insurance Market Insights 2018).

[1] Aon. Cyber Insurance Market Insights, 2018.

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

The recent enforcement of the Notifiable Data Breach (NDB) scheme as well as the recently introduced APRA CPS 234 regulation are positive steps towards improving the resilience of Australian businesses to cyber threats. However, more information on breach frequency and severity needs to be shared with the insurance industry to assist in understanding frequency/ severity relationships underpinning risk transfer policies and to educate businesses and the community on the value of taking up cyber insurance.

Such governmental regulations have already proven effective for other countries and regions. In the case of the US, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Federal Information Security Management Act (FISMA) form the three pillars for digital security compliance for businesses and governmental institutions.

Corresponding regulations for Australia is framed through the Privacy Act 1988 and subsequent amendment such as the NDB in 2017. However, compliance alone does not ensure resilience as shown by high profile cases such as the Target breach. At the end of 2013, Hackers exfiltrated more than 100 million records containing credit card details and other Personally Identifiable Information (PII) from Target's internal network. Target was PCI compliant and deployed state-of-the-art security systems but the breach still occurred due to a third party weak link, poor network segmentation and other system misconfigurations[2]. Target also possessed cyber insurance that proved useful in offsetting some of the financial losses incurred during the post-breach response period. Therefore, a well-planned response is an equally important defence strategy and cyber insurance will go a long way to providing a better incident response and business continuity.

5. How can government maintain trust from the Australian community when using its cyber security capabilities?
   No response

6. What customer protections should apply to the security of cyber goods and services?
   No response

7. What role can Government and industry play in supporting the cyber security of consumers?
   No response

[2] Xiaokui Shu et al. Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, 2017

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?
   No response

9. Are there functions the Government currently performs that could be safely devolved to the private sectors? What would the effect(s) be?
   No response

10. Is the regulatory environment for cyber security appropriate? Why or why not?

    Response: Regulatory frameworks such as the Notifiable Data Breach primarily focus on protection of privacy. In contrast, other regulation such as the CPS 234 is more balanced due to its focus on broader information security challenges beyond the protection of PII CPS 234. While only currently enforced on APRA regulated entities, CPS 234 is applicable to other organisation and presents an encouraging point of departure to lift cyber security standards in the Australian economy. The standard is principle based and non-prescriptive, offering regulated entities scope to leverage their current investment in information security management systems (ISMS) to achieve compliance.

    The 2019 update of CPG 234 (guidance for implementation of CPS 234) includes some concrete best practices such as information to be presented to the business board tabled in Appendix H. Implementation of the standard can be assisted by taking advantage of standard cyber risk quantification framework such as Factor Analysis of Information Risk (FAIR[3]).

    The FAIR methodology is a quantitative approach that provides estimates on the frequency and severity of loss events using historical data, heuristics and expert opinions. FAIR is a time test comprehensive methodology, which provides a framework for analysing tail losses through quantitative metrics such as Value at Risk. The quantification process provides a structured approach to prioritise risk and remediate efforts based on expected reduction in potential financial loss, enabling a prudent investment culture in cyber security based on established financial management principles.

11. What specific market incentives or regulatory changes should Government consider?
    No response

12. What needs to be done so that cyber security is "built in" to digital goods and services?
    No response

[3] https://www.fairinstitute.org/about

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

13. How could we approach instilling better trust in ICT supply chains?
No response

14. How can Australia governments and private entities build a market of high quality cyber security professionals in Australia?
No response

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can these be addressed?

Response: In the insurance industry cyber risk is being broadly categorised either as affirmative (named as a risk) or silent (covered without explicit recognition of the risk as it isn't excluded). Increasingly traditional commercial general liability and property insurance policies exclude cyber risk[4] with insurers looking to provide explicit policies that are accompanied by robust risk management processes. However, there still remains significant ambiguity especially when it comes to attribution of a cyber-attack[5,6]. This means that cyber insurance is emerging as a stand-alone coverage and insurance companies with "silent cyber" built into their products are exploring ways to isolate that component. Current cyber insurance policies are covering a relatively wide range of costs depending on the level of coverage. A comprehensive cover will typically include direct costs associated with a post-breach response. The following figure shows the classification of costs due to cyber-attacks[7,8]. Costs with purple outlines are currently covered by cyber insurance policies.

[4] Sasha Romanosky et al. Content analysis of cyber insurance policies: how do carriers price cyber risk?, 2019
[5] Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.
[6] Milton Mueller et al. Cyber Attribution: Can a New Institution Achieve Transnational Credibility?, 2019
[7] The Council of Economic Advisers. The cost of Malicious Cyber Activity to the U.S. Economy, 2018
[8] Deloitte. Beneath the surface of a cyberattack, 2016

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

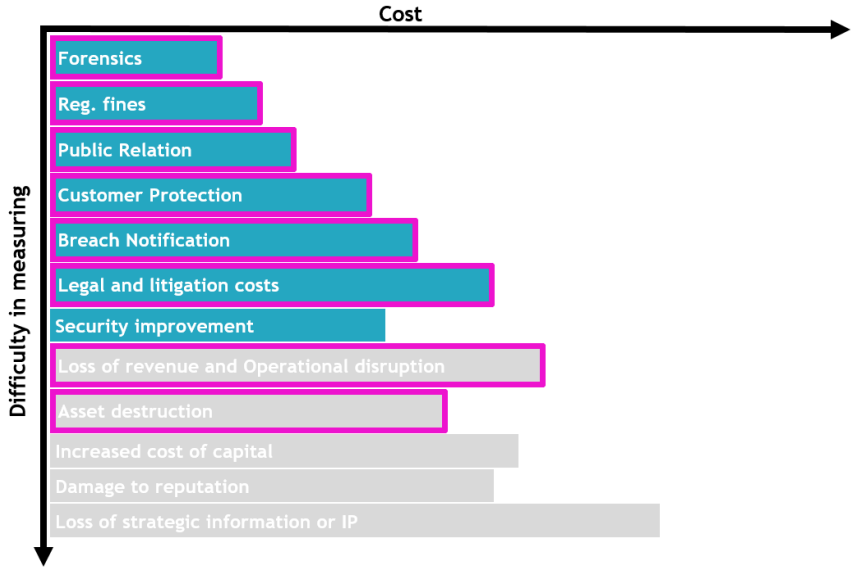

Figure 2: Costs of a cyber-security breach (Source: Risk Frontiers in-house analysis).

The first obvious observation here is that current coverage is restricted to direct costs and excludes intangible losses or long term impacts such as reputational damage. One example is the 2017 Equifax data breach where losses in market share prices and subsequent security improvements were not covered by their insurance policy.

Another barrier for the growth of cyber insurance in Australia, and globally, is that cyber risk not well understood. Brokers and underwriters lack the training and tools to quantify this emerging risk efficiently. In fact, current approaches to assessing cyber security risk rely heavily on manual assessments that greatly impede the scalability to small and medium enterprises. Unlike other mature risks such as those arising from natural catastrophes, cyber security risk is extremely hard to quantify due to its dynamic nature, the scale, the lack of physical boundaries upon which accumulations are analysed and the aggregate expertise required to produce a good model of the risk. This gap in cyber risk modelling has a major impact on pricing where premium prices becomes unsound or unaffordable for SMEs.

Another issue with current cyber insurance is regarding policy terms which drives the lack of certainty in successful claims. Since cyber insurance products are still young compared to P&C insurance, the policy terms are constantly being tested in court and usually contain explicit exclusion clauses for cases such as "act of war"[9]. A recent example of a more subtle exclusion occurred in the court case confronting National Bank of Blacksburg to its insurer Everest National Insurance Company[10].

[9] Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.
[10] https://krebsonsecurity.com/wp-content/uploads/2018/07/1-main.pdf

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

The above issues and challenges can be addressed (at least partly) through:

a. Governmental initiatives including the development of a compelling regulatory framework for cyber security risk as well as the promotion of the cyber risk management with particular emphasis on cyber insurance.
b. The government should encourage and support collaboration between academia and the industry into paving the way towards better understanding and modelling of the cyber-security risk landscape as it pertains to Australian businesses. Without a proper understanding of the risk, there is only a small degree of price differentiation across different firms.
c. The government also needs to work with insurers to assist in the "attribution" process (which is important for certain policy exclusions) and potentially consider establishing a cyber re-insurance pool.
d. Finally, the government should increase awareness and provide platforms for SMEs to explore their alternatives in terms of cyber risk transfer.

16. How can high-volume, low sophistication malicious activity targeting Australia be reduced?

Response: The first and foremost protection against high-volume and low sophistication threats is the adoption of good cyber hygiene. Credential management (password usage, multi-factor authentication for example), regular patching and employee training (resilience against phishing and scams) are amongst the top low-cost but high return strategies to prevent attacks in this category. These type of attacks are most prevalent for lower-tier enterprises which should be encouraged and made aware of the impact of good cyber hygiene. This cyber security strategy mirrors the public health management strategy in encouraging hand sanitation to minimise the spread of common cold and flu viruses that help to prevent flu pandemics. Through insurance engagement, the insurance industry can provide the services as part of a broader product offering to increase cyber hygiene.

Insurers have a vested interest in encouraging policyholders to improve their cyber resilience and incident response readiness. These initiatives improve vigilance against signs of cyber attacks and help to contain the potential financial loss from early detection and intervention. Discount in policy premium is often offered as an incentive to policyholder to implement these initiatives. For example the Marsh Cyber Catalyst program offers enhanced terms and condition as an incentive. These subsidy schemes are expensive to the insurer but with no simple way to measure the business benefit empirically. Macquarie University collaborated with Agile Underwriting in research for a new smart incentive scheme where policyholder is rewarded with reduction up to 50% of the claim excess if they develop an incident response plan using free template from the Office of the

Australian Information Commissioner (OAIC) under the Notifiable Data Breach (NDB) scheme. The benefit of this approach is in eliminating the upfront cost to the insurer by replacing premium discount with a reduction in claim excess. The availability of an incidence response plan will accelerate the incident response process and reduce the expected financial loss to the policyholder and total claim to the insurer. This scheme sustainable and self-funded through the expected reduction in claim.

17. What changes can Government make to create a hostile environment for malicious cyber actors?
No response

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?
No response

19. What private networks should be considered critical systems that need stronger cyber defences

Response: One particular critical infrastructure that has been proven accessible to cyber-attack is the electricity production and distribution system. The 2016 attack on Ukraine's power grid[11] and recent much publicised US activity on Russia's power grid[12] serve as indisputable examples. The lesson here is that the protection of critical infrastructure should be a priority along with a thorough understanding of the potential impacts if subject to a successful cyber-attack[13]. Moreover, the insurance consideration regarding the protection of critical infrastructure could in principle be incorporated into the ARPC's program. ARPC is the Australian statutory body that deals with terrorist damage to commercial buildings.

20. What funding models should Government explore for any additional protections provided to the community?

Response: A cyber re-insurance pool is one form of funding that the Government should explore to improve confidence in the cyber insurance market, increase the resilience of the economy and community to cyber-attacks and more generally as signal to build market confidence. For instance in the UK, Pool Re was established by the insurance industry and the government as a reinsurance pool to protect insurance companies against large claims originating from terrorist incidents. Since 2018, Pool Re also covers cyber-terrorism[14]. Thus similar extension or more innovative

[11] Sans and E-ISAC. Analysis of the Cyber Attack on the Ukrainian Power Grid, 2015
[12] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[13] Centre for Risk Studies, University of Cambridge. Business Blackout, 2016
[14] Willis Towers Watson. Pool Re broadens its reach, 2019

Risk Frontiers
ABN 126 1644 4234
Level 8, 33 Chandos Street
St Leonards NSW 2065

approaches, such as Hiscox's cyber Insurance-Linked Securities[15], can be explored through the ARPC to cover for cyber-attacks on critical infrastructures. Risk Frontiers can provide more detail on these schemes if required.

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?
No response

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and / or market offerings?

Response: We strongly agree.

This issue is particularly prevalent for cyber insurance where poor consumer awareness regarding policy terms and exclusions which can lead to poor decision making on implementing the most fit-for-purpose cyber insurance product. One example is given by the court case between National Bank of Blacksburg and its insurer Everest National Insurance Company. In this case, the insured was covered under a Computer and Electronic Crime protection and a Debit Card rider. The former policy has a larger limit and thus would result in a larger payout. The caveat here is that the former policy also has an exclusion clause that led to a dispute between the two entities regarding which limit applies.

The lack of cyber awareness can also limits consumer choice in negotiating the right coverage for cyber insurance and selection of optional coverage and exclusions. The difficulty arises from estimating the potential financial loss arising from cyber-attacks whose frequency appear random and result in unpredictable loss amount. In the absence of better frequency-severity information based on credible statistics the modelling of this risk will be governed by the uncertainty. The apparent randomness of such attacks gives rise to some parallels between natural catastrophic (NAT CAT) risk modelling and cyber risk modelling. Risk Frontiers is a leading expert and educator in NAT CAT risk. These modelling and education efforts can help to close this consumer knowledge gap and improve their ability to make choices in cyber security investments.

23. How can increased consumer focus on cyber security benefit Australian businesses who create cyber products?

Response: A greater uptake in cyber insurance will minimize the volatility of losses due to cyber events, improve the resilience of Australian businesses to cyber incidents as well as expand the pool of data that can be used to understand the specific impacts of cyber-attacks to the Australian economy and community.

[15] Insurance Day. Hiscox plans dedicated cyber ILS fund, 2019

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?
    No response

25. Would you like to see cyber security features prioritised in products and services?
    No response

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

    No response

About the authors

Dr. Ryan Springall is General Manager at Risk Frontiers and is responsible for delivering Risk Frontiers' products and services to the (re)insurance, capital markets, banking and government sectors.

Prior to joining Risk Frontiers, Ryan was a Senior Broker and manager at Aon Japan in Tokyo from 2015. His primary professional focus was managing a team of brokers and analysts in directing risk capital strategies, transacting reinsurance and client advocacy.

Ryan was formerly a senior analyst within the Australian Defence Intelligence Organisation and was appointed General Manager of Risk Frontiers in 2019. Ryan holds a PhD in Physics.

Dr Tahiry Rabehaja is a Research Fellow at the Optus Macquarie University Cyber Security Hub and Technology Officer at Risk Frontiers. His background is in Theoretical Computer Science and Information Security. His current research area includes cyber security risk quantification.

Denny Wan is a cyber-security specialist and researcher in cyber insurance pricing strategy. He specialises in cyber risk quantification techniques based on the Open Group FAIR framework. He is a certified PCI QSA, ISO 27001 Lead Auditor and a CISSP.